

CLAIMS

What is claimed is:

- 1 1. A computer system comprising:
2 a central processing unit (CPU);
3 a chipset, coupled to the CPU, including:
4 protected registers; and
5 a host controller;
6 a bus coupled to the host controller; and
7 a peripheral device coupled the bus, wherein trusted software accesses the
8 protected registers to transmit encrypted data between the host controller and
9 the peripheral device upon startup of the computer system to verify that the
10 peripheral device is trustworthy.
- 1 2. The computer system of claim 1 wherein the encryption data is generated
2 at the peripheral device and transmitted to the host controller.
- 1 3. The computer system of claim 1 wherein the encryption data is generated
2 at the CPU and transmitted to the peripheral device.
- 1 4. The computer system of claim 1 wherein the trusted software writes to the
2 protected register to indicate to the host controller the encrypted data to transmit
3 and response data that is to be received.
- 1 5. The computer system of claim 1 wherein the chipset further comprises:
2 a protected memory table; and
3 a memory controller coupled to the memory device.
- 1 6. The computer system of claim 5 further comprising a memory device
2 coupled to the memory controller.

- 1 7. The computer system of claim 6 wherein the data transmitted between the
2 host controller and the peripheral device bypasses a stack at the memory device
3 associated with the peripheral device.
- 1 8. The computer system of claim 7 wherein the memory device comprises:
2 a protected memory table; and
3 a trusted software monitor.
- 1 9. The computer system of claim 1 wherein the peripheral device is a
2 keyboard.
- 1 10. The computer system of claim 1 wherein the peripheral device is a mouse.
- 1 11. The computer system of claim 1 wherein the peripheral device is a
2 scanner.
- 1 12. The computer system of claim 1 wherein the bus is a Universal Serial Bus.
- 1 13. A chipset comprising:
2 protected registers; and
3 a host controller coupled to a peripheral device via a bus;
4 wherein trusted software accesses the protected registers to transmit
5 encrypted data between the host controller and the peripheral device to verify
6 that the peripheral device is trustworthy.
- 1 14. The chipset of claim 13 wherein the encryption data is generated at the
2 peripheral device and transmitted to the host controller.
- 1 15. The chipset of claim 13 wherein the encryption data is received from a
2 CPU coupled to the chipset and transmitted to the peripheral device.

1 16. The chipset of claim 13 wherein the trusted software writes to the
2 protected register to indicate to the host controller the encrypted data to transmit
3 and response data that is to be received.

1 17. The chipset of claim 13 wherein the chipset further comprises:
2 a protected memory table; and
3 a memory controller coupled to the memory device.

1 18. A method comprising:
2 generating an encryption key within a computer system using trusted
3 software;
4 the trusted software writing to trusted registers within the computer
5 system to initiate transmission of the encrypted key to a peripheral device; and
6 transmitting the encryption key to the peripheral device.

1 19. The method of claim 18 wherein the encryption key is transmitted to the
2 peripheral device while bypassing a memory stack associated with the
3 peripheral device.

1 20. The method of claim 18 further comprising verifying whether the
2 peripheral device is operating based upon the encryption key.

1 21. A computer system comprising:
2 a central processing unit (CPU);
3 a chipset, coupled to the CPU, including:
4 protected registers; and
5 a host controller;
6 a memory device coupled to the chipset;
7 a bus coupled to the host controller; and

8 a peripheral device coupled the bus, wherein trusted software accesses the
9 protected registers to transmit encrypted data between the host controller and
10 the peripheral device upon startup of the computer system to verify that the
11 peripheral device is trustworthy.

1 22. The computer system of claim 21 wherein the encryption data is generated
2 at the peripheral device and transmitted to the host controller.

1 23. The computer system of claim 21 wherein the encryption data is generated
2 at the CPU and transmitted to the peripheral device.

1 24. The computer system of claim 21 wherein the trusted software writes to
2 the protected register to indicate to the host controller the encrypted data to
3 transmit and response data that is to be received.

1 25. The computer system of claim 21 wherein the chipset further comprises:
2 a protected memory table; and
3 a memory controller coupled to the memory device.

1 26. The computer system of claim 21 wherein the data transmitted between
2 the host controller and the peripheral device bypasses a stack at the memory
3 device associated with the peripheral device.

1 27. The computer system of claim 21 wherein the memory device comprises:
2 a protected memory table; and
3 a trusted software monitor.

1 28. The computer system of claim 21 wherein the peripheral device is a
2 keyboard.

1 29. The computer system of claim 21 wherein the peripheral device is a
2 mouse.

1 30. The computer system of claim 21 wherein the peripheral device is a
2 scanner.

1 31. The computer system of claim 21 wherein the bus is a Universal Serial
2 Bus.